Владимир ШИЛИН
руководитель дирекции системных проектов АО «РНТ», кандидат технических наук

Роман КОЗЫРЬ
эксперт по информационной безопасности АО «РНТ»

ЗАКОН В ТРЕНДЕ

187-ФЗ И ЕГО ПРИМЕНИМОСТЬ В БАНКОВСКОЙ СФЕРЕ

С 1 января 2018 года вступил в силу Федеральный закон от 26.07.2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Закон направлен на реализацию мер защиты IT-систем государственных и коммерческих организаций, сбои в работе которых могут привести к тяжёлым социальным, политическим, экономическим, экологическим последствиям, а также помешать обеспечению обороноспособности, безопасности государства и правопорядка. В число сфер деятельности, участники которых указаны в законе как субъекты критической информационной инфраструктуры (КИИ), включены банковская и иные сферы финансового рынка. Согласно указанному в Постановлении Правительства РФ № 127 от 08.02.2018 г. перечню показателей критериев значимости объектов КИИ, значительное число банков относятся к субъектам КИИ и будут обязаны выполнять требования 187-ФЗ.

За неисполнение требований 187-ФЗ предусмотрена ответственность для организаций и ответственных лиц, вплоть до уголовной.

ЭТАПЫ РЕАЛИЗАЦИИ 187-ФЗ

Закон подразумевает поэтапную реализацию его требований, которые мы рассмотрим далее.

Первый этап включает определение принадлежности организации к субъектам КИИ. Реализация возложена на саму организацию, в рамках которой необходимо составить перечень IT-систем (информационных систем), участвующих в деятельности банковской и иных сферах финансового рынка.

Вторым этапом необходимо провести категорирование объектов КИИ в соответствии с ПП РФ № 127. Реализация также возложена на саму организацию, включает в себя создание комиссии по категорированию, определение перечня процессов деятельности организации и выявление критических процессов, разработку перечня объектов КИИ, подлежащих категорированию, определение угроз безопасности и категории значимости для объектов КИИ. Критерии значимости объектов КИИ, напрямую касающиеся банковской сферы, указаны в п. 10 Перечня показателей критериев, утверждённых ПП № 127. В организациях, например, кредитно-финансовой сферы, возможно, потребуется рассмотрение и других критериев из ПП № 127. После этого подготовленный список объектов КИИ по форме, определённой в Информационном сообщении ФСТЭК России от 24 августа 2018 г. № 240/25/3752, необходимо направить во ФСТЭК России. Затем, после подготовки материалов по форме, предусмотренной Приказом ФСТЭК России № 236 от 22.12.2017 г., сведения о категорировании необходимо направить во ФСТЭК России, причём в случае отсутствия необходимости присвоения объектам одной из трёх категорий согласно ПП № 127, ФСТЭК также необходимо уведомить об этом.

В случае отсутствия у организации квалифицированных кадров для выполнения вышеуказанных этапов, возможно привлечь к этому сторонние организации, обладающие достаточной квалификацией, в частности АО «РНТ».

Третий этап заключается в создании или модернизации системы защиты объектов КИИ в соответствии с требованиями приказов ФСТЭК России № 235 от 21.12.2017 г., № 239 от 25.12.2017 г. и при необходимости — № 138 от 09.08.2018 г. Данный этап выполняется подразделением ИБ организации и лицензиатом ФСТЭК России по технической защите конфиденциальной информации. Весь комплекс работ включает в себя подэтапы, указанные ниже:

- Разработка требований к обеспечению безопасности объектов КИИ. Для этого необходимо провести обследование IT-систем объектов КИИ и анализ возможных угрозы согласно присвоенным им категориям.
- Разработка технического задания на создание системы защиты. В нем определяются требования конкретно к системе защиты, основанные на предыдущем подэтапе, с учётом положений организационно-распорядительных документов по безопасности объектов КИИ, а также требования по взаимодействию с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) в соответствии с приказами ФСБ России № 367 и № 368 от 24.07.2018 г.
- Разработка организационных и технических мер по обеспечению безопасности объекта КИИ. На данном подэтапе определяются адекватные средства защиты для объекта КИИ и необходимый комплект документации в соответствии с требованиями приказа ФСТЭК России № 239 от 25.12.2017 г. Далее происходит проектирование системы безопасности и разрабатывается эксплуатационная документация.
- Внедрение организационных и технических мер защиты. На этом подэтапе проводятся работы по внедрению системы безопасности и обучение ответственных сотрудников. При необходимости перед внедрением проводятся испытания выбранных средств защиты на специальном стенде с целью убедиться, что средства защиты не создадут проблем функционирования защищаемых объектов КИИ по их основному профилю. Также организуется взаимодействие с ГосСОПКА в соответствии с разработанными ранее требованиями.
- Опытная эксплуатация и аттестация объекта КИИ. Во время опытной эксплуатации проверяется стабильность работы защищённых IT-систем и самой системы защиты. По её результатам система защиты либо дорабатывается, либо принимается, и проводится ее аттестация на соответствие требованиям по обеспечению информационной безопасности.

Также можно обозначить, условно, **четвёртый этап** — сопровождение созданной системы защиты. Он включает в себя техническую поддержку средств защиты и актуализацию документации и настроек в случае изменений в работе защищаемых IT-систем объектов КИИ. Это осуществляется либо сотрудниками самой организации, либо специализированной организацией на аутсорсинге.

ОБ ОТВЕТСТВЕННОСТИ

Стоит ещё раз упомянуть об ответственности для организаций — субъектов КИИ. Федеральным законом № 194-ФЗ от 26.07.2017 г. в УПК РФ внесены изменения в связи с принятием 187-ФЗ. В главу 28 УК РФ добавлена статья 274, подпункты 3, 4, 5 которой касаются субъектов КИИ и их ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом информации, содержащейся в КИИ, либо правил доступа, если оно повлекло причинение вреда для КИИ. Также за несвоевременное предоставление информации во ФСТЭК России по первым двум этапам предусмотрена ответственность по ст. 19.5 КоАП РФ.

ВЫГОДА

Общий вывод из вышеуказанного следующий: несмотря на затраты на реализацию требований закона, итоговую выгоду можно получить в виде минимизации простоя сервисов из-за компьютерных атак и обеспечения непрерывности бизнеса. Также выполнение 187-ФЗ снимет большинство вопросов проверяющих органов в части выполнения требований федеральных органов исполнительной власти.

ЕСЛИ ТРЕБУЕТСЯ ПОМОЩЬ

Весь комплекс услуг по аудиту IT-систем и подготовке проектов документов по их принадлежности к КИИ и категорированию, проектированию, осуществлению поставок средств защиты и проведению работ по их внедрению, разработку всей необходимой документации, а также аттестацию и последующее сопровождение систем защиты объектов КИИ может провести АО «РНТ», обладающее достаточным штатом квалифицированных специалистов и всеми необходимыми лицензиями на данные виды деятельности.

* * *

В заключение необходимо сказать, что сроки реализации требований закона на момент написания этой статьи следующие: выполнение первых двух этапов согласно ПП № 127 предполагается до 20.02.2019 г., после чего, согласно рекомендациям ФСТЭК России, создание систем безопасности значимых объектов КИИ должно пройти до 01.09.2019 г. Однако сейчас идёт активная работа по формированию итогового текста проекта по внесению изменений в ПП № 127, который также повлияет и на сроки. В текущем проекте срок выполнения первого этапа указан до 01.06.2019 г., второго этапа — не позднее 6 месяцев со дня окончания первого этапа в самой организации. Скорее всего, изменения в ПП № 127 будут приняты, и время, данное для определения и категорирования объектов КИИ, будет продлено.